UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,585	03/29/2004	Jeffrey A. Aaron	BELL-0340/00379 C1	2073

39072 7590 06/20/2006

MYERS BIGEL SIBLEY & SAJOVEC, P.A.
P.O. BOX 37428
RALEIGH, NC 27627

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/811,585	AARON ET AL.	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *23-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *23-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/19/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on 03/29/04.

2. Claims 23-42 are under examination.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 23, 24-28, 29-34, 35, 36-42 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 3-7, 9-14, 17, 26-32 of U.S. Patent No. 6,715,084. Although the conflicting claims are not identical, they are not patentably distinct from the earlier patent claim and as such are unpatentable for obvious-type double patenting.

Claims 1, 3-7, 9-14, 17, 26-32 of U.S. Patent No. 6,715,084 contain every element of claim 23, 24-28, 29-34, 35, 36-42 of the instant application and thus anticipate the claims of the instant application. Claims of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a 35 patent claim to a species within that genus). "ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001). "Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is **"anticipated"** by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4 . This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic application. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982); Schneller, 397 F.2d at 354. Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting." (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 23-29, 32-41 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) and Shipley (US Patent No. 6,119,236).

As per claim 23, Aucsmith teaches:

determining that the device is anticipated to be affected by an anomaly by using network-based intrusion detection techniques [paragraph 0044, 0045, 0048 lines 1-4, paragraph 0049] and sending an alert to the device that the anomaly is anticipated at the device [paragraph 0051].

Aucsmith teaches that comparing the anomaly with information previously logged at the server (e.g. security data, intrusion pattern, non-standard access pattern etc.). Aucsmith doesn't expressively mention that analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system.

However, Shipley teaches that analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system and by using pattern correlations

across the plurality of hosts, servers, and computer sites [Fig. 1, 2, col. 5 lines 51-62, col. 6 lines 4-14].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Shipley with Aucsmith to analyzing the data entering into the networked computer system, since one would have been motivated to prevent the unauthorized intrusion into the computer networks and to control network firewall [Shipley, col. 1 lines 15-16, col. 3 line 23].

As per claim 24, the rejection of claim 23 is incorporated and Aucsmith teaches:

adjusting a firewall of the device that is anticipated to be affected by the anomaly [paragraph 0054, Fig. 1].

As per claim 25, the rejection of claim 23 is incorporated and Aucsmith teaches:

the anomaly comprises one of an intrusion and an intrusion attempt [paragraph 0027 lines 7-17].

As per claim 26, the rejection of claim 23 is incorporated and Shipley teaches:

analyzing a plurality of data packets with respect to predetermined patterns [col. 5 lines 52-53, Fig. 2].

As per claim 27, the rejection of claim 26 is incorporated and Aucsmith teaches:

analyzing data packets that have been received by at least two devices in the networked computer system [Fig. 1].

As per claim 28, the rejection of claim 23 is incorporated and Aucsmith teaches: recognition of an intrusion and further comprising generating an automated response to the intrusion [paragraph 0048 lines 1-4, paragraph 0051, 0055 lines 1-12, paragraph 0056 lines 3-6].

As per claim 29, Aucsmith teaches:

detecting an anomaly at a first device in the computer system using network-based intrusion detection techniques [paragraph 0039];

determining a device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites [Fig.1, paragraph 0043, 0045, 0048 lines 1-4, 0049, 0055 lines 1-4].

Aucsmith teaches that comparing the anomaly with information previously logged at the server (e.g. security data, intrusion pattern, non-standard access pattern etc.). Aucsmith doesn't expressively mention that analyzing *data entering into a plurality* of hosts, servers, and computer sites in the networked computer system.

However, Shipley teaches that analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system and by using pattern correlations across the plurality of hosts, servers, and computer sites [Fig. 1, 2, col. 5 lines 51-62, col. 6 lines 4-14].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Shipley with Aucsmith to analyzing the data entering into the networked computer system, since one would have been motivated to prevent the unauthorized intrusion into the computer networks [Shipley, col. 1 lines 15-16, col. 3 line 23].

As per claim 32, the rejection of claim 29 is incorporated and Aucsmith teaches:
the anomaly comprises one of an intrusion and an intrusion attempt [paragraph 0027 lines 7-17].

As per claim 33, the rejection of claim 29 is incorporated and Shipley teaches:
analyzing a plurality of data packets with respect to predetermined patterns [col. 5 lines 52-53, Fig. 2].

As per claim 34, the rejection of claim 33 is incorporated and Aucsmith teaches:
analyzing data packets that have been received by at least two devices in the networked computer system [Fig. 1].

As per claim 35, the rejection of claim 29 is incorporated and Aucsmith teaches:
controlling the device that is anticipated to be affected by the anomaly [paragraph 0054, 0057, Fig. 1].

As per claim 36, Aucsmith teaches:

a data collection and processing center [Fig. 1, component 104] monitoring data communicated to a network [Fig. 1], and detecting an anomaly in the network using network-based intrusion detection techniques [paragraph 0044, 0045, 0048 lines 1-4, paragraph 0049].

Aucsmith teaches that comparing the anomaly with information previously logged at the server (e.g. security data, intrusion pattern, non-standard access pattern etc.) [paragraph 0045 lines 4-5]. Aucsmith doesn't expressively mention that analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system.

However, Shipley teaches that analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system [Fig. 1, 2, col. 5 lines 51-62, col. 6 lines 4-14].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Shipley with Aucsmith to analyzing the data entering into the networked computer system, since one would have been motivated to prevent the unauthorized intrusion into the computer networks and to control network firewall [Shipley, col. 1 lines 15-16, col. 3 line 23].

As per claim 37, the rejection of claim 36 is incorporated and Aucsmith teaches:

the data collection and processing center determines which of a plurality of devices that are connected to the network are anticipated to be affected by the anomaly by using

pattern correlations across the plurality of hosts, servers, and computer sites, and alerting the devices [Fig.1, paragraph 0043, 0045, 0048 lines 1-4, 0049, 0055 lines 1-4, paragraph 0035].

As per claim 38, the rejection of claim 36 is incorporated and Aucsmith teaches:
the data collection and processing center further determines which of a plurality of devices that are connected to the network have been affected by the anomaly and alerts the devices [Fig.1, paragraph 0043, 0045, 0048 lines 1-4, 0049, 0055 lines 1-4, 0051, 0052, paragraph 0035].

As per claim 39, the rejection of claim 36 is incorporated and Aucsmith teaches:
the data collection and processing center further adjusts a firewall of each of a plurality of devices that is connected to the network that is anticipated to be affected by the anomaly responsive to the detection of the anomaly [Fig.1, paragraph 0054].

As per claim 40, the rejection of claim 36 is incorporated and Aucsmith teaches:
the anomaly comprises one of an intrusion, an intrusion attempt and reconnaissance activity [paragraph 0027 lines 7-17].

As per claim 41, the rejection of claim 36 is incorporated and Shipley teaches:
analyzing a plurality of data packets with respect to predetermined patterns [col. 5 lines 52-53, Fig. 2].

As per claim 42, the rejection of claim 41 is incorporated and Aucsmith teaches: analyzing data packets that have been received by at least two devices that are connected to the network [Fig. 1].

5. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) Shipley (US Patent No. 6,119,236) and in view of Bondi (US Patent No. 5,710,885).

As per claim 30, the rejection of claim 29 is incorporated and Shipley teaches a plurality of devices [Fig. 1], the first device being polled prior to detecting the anomaly [Fig.1, 2, col. 5 lines 52-54, col. 7 lines 51-58 col. 8 lines 18-25]. Aucsmith teaches that the first device being polled prior to detecting the anomaly, and the device anticipated to be affected by the anomaly is a device that has not been polled [Fig. 1, paragraph 0013]. Aucsmith and Shipley don't expressively mention the plurality of devices are *polled in a predetermined sequential order.*

However, Bondi teaches the plurality of devices are polled in a predetermined sequential order [col. 3 lines 31-40].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Bondi with Aucsmith and Shipley, since one would

have been motivated to prevent the unauthorized intrusion into the computer networks [Shipley, col. 1 lines 15-16].

6. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) Shipley (US Patent No. 6,119,236) and in view of Wolff et al. (US Pub. No. 2002/0174358).

As per claim 31, the rejection of claim 29 is incorporated and Aucsmith teaches that transmitting an anomaly warning from the first device to a central analysis engine, responsive to detecting the anomaly at the first device [Fig. 1, paragraph 0041 lines 1-5]. Aucsmith doesn't expressively mention that warning comprising a unique device identifier.

However, Wolff teaches that warning (i.e. report) comprising a unique device identifier [paragraph 0017 lines 1-4].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wolff with Aucsmith and Shipley, since one would have been motivated to obtain accurate picture of anomaly and to identify a particular event and a device [Wolff, paragraph 0005 lines 1-2, 0010 lines 1-2].

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sheikh et al (US 2002/0078382) --- Scalable system for monitoring network system and components and methodology therefore.

Bunker V. et al (US 2003/0009696) --- Network security testing.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP

6/8/06

HOSUK SONG
PRIMARY EXAMINER